INSIGHT QUANTUM COMPUTING NEWS

Is RSA-2048 already broken?

No. No quantum computer today can break RSA-2048. But the estimated machine needed keeps shrinking, and NIST has set end dates for RSA whatever the key size.



Carlos E. Avimadjessi
CTO, Co-Founder · CISSP, CCSP, CISM
Reviewed by Sokaïna Jabbar

PUBLISHED	LAST REVIEWED	READING TIME
24 November 2026	24 November 2026	3 min

SHORT ANSWER

No. No quantum computer today can break RSA-2048, and NIST confirmed in October 2026 that no cryptanalytically relevant quantum computer exists yet. But the estimated size of the machine needed fell from 20 million noisy qubits in 2019 to under one million in 2025, and NIST will deprecate RSA after 2030 and disallow it after 2035, whatever the key size.

© 2026 Sorlos

Why the question comes up now

Each announcement of a new quantum processor brings the same question from boards and clients: is the encryption we use still safe? RSA-2048 is the usual example, because it protects a large share of today's certificates, signatures and key exchanges. In October 2026, NIST published the final version of its transition plan, which turns the answer into dates.

What it would take to break RSA-2048

RSA is safe against ordinary computers: NIST rates RSA-2048 at 112 bits of classical security, enough for it to stay approved until 2030. The risk comes from Shor's algorithm, which can factor large numbers efficiently on a large enough quantum computer. NIST describes RSA and elliptic-curve cryptography as "vulnerable to Shor's Algorithm on a cryptanalytically relevant quantum computer".

How large is large enough? The best published estimates come from Craig Gidney of Google Quantum AI:

Published estimates of the quantum computer needed to factor RSA-2048

ESTIMATE	NOISY QUBITS	TIME TO FACTOR ONE KEY
Gidney and Ekerå, 2019	20 million	About 8 hours
Gidney, 2025	Under 1 million	Under a week

Both estimates assume a machine where one gate operation in a thousand fails and error correction runs every microsecond. No machine of that size exists today. The 2025 paper did not bring the machine closer; it showed that a much smaller machine would be enough. Gidney writes that he does not expect such machines to exist by 2030, but that security should not depend on progress staying slow.

Why "not broken" does not mean "safe"

Three reasons make the question less comforting than the answer.

- **Data can be recorded now.** An attacker can store encrypted traffic today and decrypt it once a quantum computer exists. This is harvest now, decrypt later, and it matters most for data that must stay confidential for years.
- **The estimates keep falling.** In the Global Risk Institute's yearly survey, published in March 2026, experts consider a quantum computer able to break today's public-key cryptography "quite possible" within 10 years (28 to 49%) and "likely" within 15 years (51 to 70%).

- **The end dates are set.** NIST "will deprecate all quantum-vulnerable digital signature algorithms after 2030 and disallow their use under NIST standards and guidelines after 2035", and applies the same dates to key establishment. Its tables list RSA at both 112 and 128 bits of security: a longer key does not change the dates.

What it means for your organisation

1. **Don't panic, and don't wait.** RSA-2048 is not broken today. Migration takes years, so the time to plan is now, not when a breakthrough is announced.
2. **Don't plan on longer RSA keys.** Moving from RSA-2048 to RSA-4096 does not protect against a quantum computer, and NIST's dates apply to both. Plan for post-quantum algorithms such as ML-KEM instead.
3. **Find where you use RSA and elliptic curves.** Certificates, VPNs, signatures on software and documents, and key exchanges in TLS. Our article What is a cryptographic inventory, and where do you start? explains how.
4. **Protect long-lived data first.** Key exchange is the priority because of harvest now, decrypt later. A hybrid key exchange adds post-quantum protection while keeping a classical algorithm.
5. **Write down your assumption about timing.** Our article What is the Mosca inequality? shows how to turn it into a priority list.

Sources

1. National Institute of Standards and Technology (US), Transition to Post-Quantum Cryptography Standards (NIST IR 8547), 27 October 2026.
   https://csrc.nist.gov/pubs/ir/8547/final
2. Craig Gidney and Martin Ekerå, Google and KTH Royal Institute of Technology, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, 23 May 2019.
   https://arxiv.org/abs/1905.09749
3. Craig Gidney, Google Quantum AI, How to factor 2048 bit RSA integers with less than a million noisy qubits, 21 May 2025.
   https://arxiv.org/abs/2505.15917
4. Michele Mosca and Marco Piani, Global Risk Institute and evolutionQ, Quantum Threat Timeline Report 2025, 9 March 2026.
   https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

AI tools assisted with the research, drafting and fact-checking of this article. The author wrote and approved the final text, and a second reviewer checked every source against the original.

Need assistance for your transition?

Sorlos runs quantum readiness assessments. We assess your risk from your cryptographic inventory and design a migration roadmap you can rely on. Vendor-independent, from Brussels.

Talk to us · www.sorlos.eu/#contact



Carlos E. Avimadjessi

Experienced Information Security Manager and Consultant. Carlos brings extensive expertise in managing security posture, risk, compliance, and operations for major enterprise and public-sector clients.

This PDF reproduces the article as of 24 November 2026. The online version, kept up to date, is at https://www.sorlos.eu/insights/is-rsa-2048-already-broken/. © 2026 Sorlos. All rights reserved.